

Russian Cyber Actors and Islamic State in Iraq and Syria

Are there interaction on the Deep and Dark Web?

White Canvas Group

Fall 2016

N0001416P3021

POC – Timothy Newberry

tim@whitecanvasgroup.com

Abstract

Research concerning Russian Cyber Actors and the Islamic State of Iraq and Syria on the Deep and Dark Web remains limited due to the complexity and difficulty of conducting research in the unindexed hidden layers of the Internet. This research paper is intended to illuminate possible interactions between Russian Cyber Actors and Islamic State in Iraq and Syria's (ISIS) cyber activity on the Deep and Dark Web with a focus on the United Cyber Caliphate using publicly available information.

Despite various open source claims and related conjecture, our research during the fall of 2016 time period concludes that there are little or no discoverable and direct publicly available communications between 'Russian Cyber Actors' and 'ISIS' and further, that there are similar yet different behaviors and traits that distinguish the two acting bodies. Related to this, there are indications that ISIS is passively monitoring Russian practices to emulate Russian activity, enhance cyber skills, and establish a true United Cyber Caliphate with advanced capabilities.

Russian Cyber Actors and Islamic State in Iraq and Syria Interaction on the Deep and Dark Web

The global spectrum of conflict in 2016 and going into 2017 includes – unfortunately – many events and areas of interest from the South China Sea, to the southern Border of the United States, and finally to the ongoing Civil War in Syria with relation to Islamic State in Iraq and Syria (ISIS), Turkey, Syria, and Russia, among others. Our research, with focus on the Syrian conflict and the cyber information battlefield, aimed to illuminate information around the relationship, or not, between Russia and ISIS cyber capability providers after various open source reports alluded to direct ties between the ISIS online footprint and Russia (intelNews | “Islamic State’s online army is a Russian front, says German intelligence”, 2016).

Research concluded there are no direct ties between Russian cyber actors, state-sponsored or otherwise and ISIS. Additionally, research demonstrates there are no direct ties with ISIS-affiliated cyber actors or a topically affiliated group, the United Cyber Caliphate. No direct ties could be identified using publicly available information that other than unconfirmed open source news media. Therefore, it was important to take additional steps and assess the utilization of the Deep and Dark Web among various groups with Russian affiliation; such groups are also likely to use these areas of the internet for illicit activity (Dishman, 2016). There are, however, indications that ISIS affiliated cyber actors are passively monitoring Russian activity to possibly establish their own robust United Cyber Caliphate to conduct cyber jihad (reference the Appendix for definitions).

Research Domain - Defining the Layers of the Internet

The size of the Internet and data contained within its three layers (clear net, deep and dark web/nets) is immeasurable as the vast majority of data is not indexed and hidden within the layers known as the Deep and Dark Webs. Before a thorough analysis may be carried out, we must clearly define what each layer of the Internet is, how to get there, and the unique characteristics and purposes that drive cyber actors to use any particular layer. As the below table depicts, there are three layers of the Internet: The Clear Web, the Deep Web, and the Dark Web, each with its own unique characteristics and use as depicted in Table 1 (ref: Appendix).

| Type | Characteristics | Access | Reasons for Use - Normal Activity |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Clear Web or Surface Web | <ul style="list-style-type: none"> • Largely indexed and easily navigable | <ul style="list-style-type: none"> • Search Engines: Google, Bing, Yahoo, Duck-Duck-Go, etc. • Direct URLs | <ul style="list-style-type: none"> • Everyday searches and everyday information: “Google it” • “How is the weather in Washington DC?” • Online shopping and purchasing |
| Deep Web | <ul style="list-style-type: none"> • Restricted Access • Partially indexed • Connected to Clear Web interfaces | <ul style="list-style-type: none"> • Username and Password protected sites • Blogs and forums that require registration • Mobile applications | <ul style="list-style-type: none"> • Financial and Banking data • Chatrooms • Blogs |
| Dark Web | <ul style="list-style-type: none"> • Not indexed by traditional search engines • Peer-to-peer • Can be connected to Clear Web interfaces • Alphanumeric URLs ending with .onion, .i2p, .bit, .onion.to • Known as the “internet on top of the internet” • Thought of as a place for illegal/illicit activity, but not always the case | <ul style="list-style-type: none"> • Requires special software and network configurations: The Onion Router (TOR), I2P, Freenet, Zeronet, Tor2Web | <ul style="list-style-type: none"> • Forums • Blogs • Security and anonymity-conscious personnel hosting websites and information • Marketplaces, Bitcoin services, hitman services, pornography, hacker chatrooms, hacker forums, email services, fraudulent documents, financial documents, weapons, torrents...etc. |

Table 1. Description of Web Layers

Scoping the Research Area - Assessing the Ties between Russia and ISIS

For reasons of national security, it is important to continue to monitor the passive, possibly indirect, relationship between Russia and ISIS, as the latter appears to be making strides towards improvements in their cyber capability and truly establishing what is known as the United Cyber Caliphate. To assess the presence of ties between Russian cyber actors and ISIS Cyber actors, and between July and December of 2016, we conducted research across 289 Deep and Dark Web forums; all found to have differing uses connected to both legitimate and illicit internet activity. As shown in Image 1 below, we have outlined the three cyber-groups of interest for this research to include the United Cyber Caliphate, ISIS “Hackers”, and Russian “Hackers”. The following pages provide more detailed analysis on each of these three demographics and the interactions or behaviors between them.

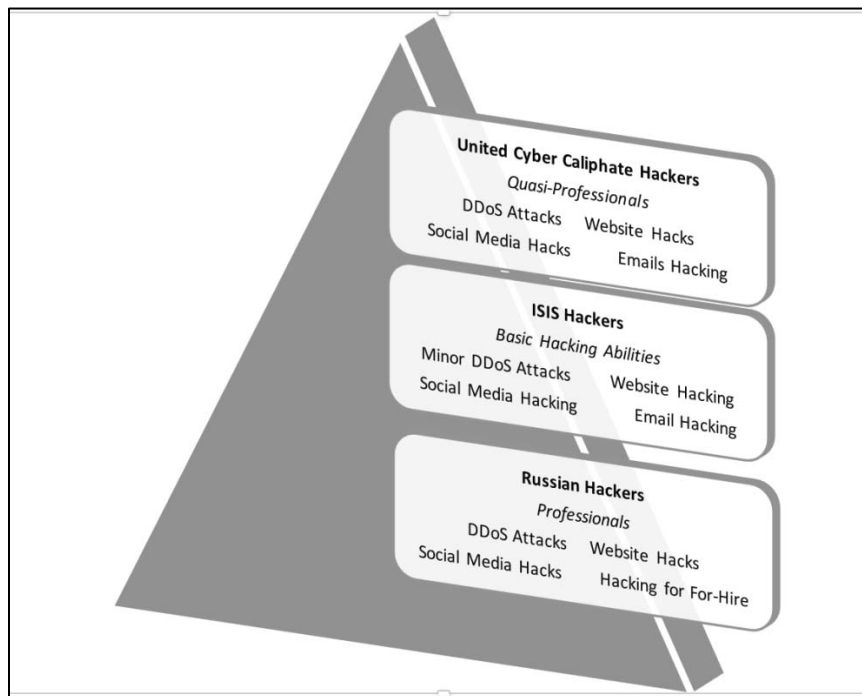


Image 1: Comparison of Activities on the Deep and Dark Web

Each of the groups has a vested interest in hacking. Whether this activity is in performing Distributed Denial of Service (DDoS) attacks or simply hacking email and social media accounts for propaganda reasons, information sharing, or command and control methods, all groups continue to disrupt every day activity and illegally obtain data through hacking to support their specific agendas (ref: Appendix).

Russia: Cyber Deep and Dark Web Trends

The Russian use of disinformation campaigns took shape in the 1960s with Soviet tradecraft known as *dezinformatsiya*, the injection of false information with the intent to deceive public opinion. Disinformation operations differ from conventional propaganda in that their origin and activity usually involve some form of clandestine action (Barron, 1974). The disinformation campaign, employed by the Soviets has now morphed into a very powerful and extensive cyber disinformation campaign present in the digital domain (ref: Appendix).

This campaign seems to have first appeared in 2003 with various stories published in Russia. The earliest documented allegations of the existence of online "Russian Trolls" appears to be in the April 2003 Vestnik Online article "The Virtual Eye of Big Brother" by French journalist Anna Polyanskaya (Polyanskaya, 2003). Polyanskaya was a former assistant to assassinated Russian politician Galina Starovoitova and two other authors, Andrey Krivov and Ivan Lomako.

While explicit ties between Russia's various intelligence services and hackers remain "plausibly deniable," the common belief now accepted among cyber security professionals is that Russia is employing layers of malign cyber actors with various degrees of direct control (Dayspring, 2015). On one end of the spectrum are state-run cyber-espionage organizations such as the Sofacy Group, also known as the Advanced Persistent Threat 28 or "APT 28" (Schindler,

2016). At the other end is the “volunteer hacker,” who engages in what may be called cyber-mischief, and is supportive of Russian President Putin’s goals and rhetoric (Matthews, 2015). Within this spectrum are also “cyber-mafia,” organizations which engage in any criminal behavior provided it doesn’t target Russia and focuses on Kremlin priorities and propaganda when requested (Matthews, 2015) (ref: Appendix).

One of the most influential Russian state-sponsored groups is the Web Brigades, also known as the Troll Army. The Troll Army consists of online anonymous entities acting as political commentators and linked to the Russian government. Jessikka Aro and Andre Chen (Chen, 2015), both journalists, conducted research on the Troll Army and published their findings in the New York Times. Publicly available information indicates these trolls physically work at the Internet Research Agency in Saint Petersburg, Russia in addition to other undisclosed locations (Chen, 2015). Based on observable information, as well as Tactics, Techniques, and Procedures (TTP) tracked across these different platforms, the primary mission of the Russian Web Brigades appears to revolve around maintaining an aggressive online, pro-Russian, disinformation campaign (Priest, Nakashima, & Hamburger, 2016) on the Clear Web (see Appendix for definitions).

Russian state-sponsored activity is near impossible to identify on the Deep or Dark Web as they are not the typical egotistical hackers that brag about their abilities. A small percentage of the Troll Army is presumed to be active on the forums offering their hacking skills and abilities as a service (Matthews, 2015). Our research revealed most Russian Dark Web activity is discoverable through The Onion Router (TOR) Browser with some activity found on I2P forums. Findings in Russian language pages on Dark Web forums were consistent with the findings on the Deep Web; however, we did find the Dark Web forms contain significantly more criminal

activity, such as drug and weapons sales, torrent activity, anarchist activity, and pornography. Based on our research, there was no direct information pertaining directly to state-sponsored cyber organizations activity found within Deep or Dark Web forums; not surprising considering the sophistication and guidance that is well-known from this State. Most information contained within the Deep and Dark Web provided links to Clear Web articles and news reports.

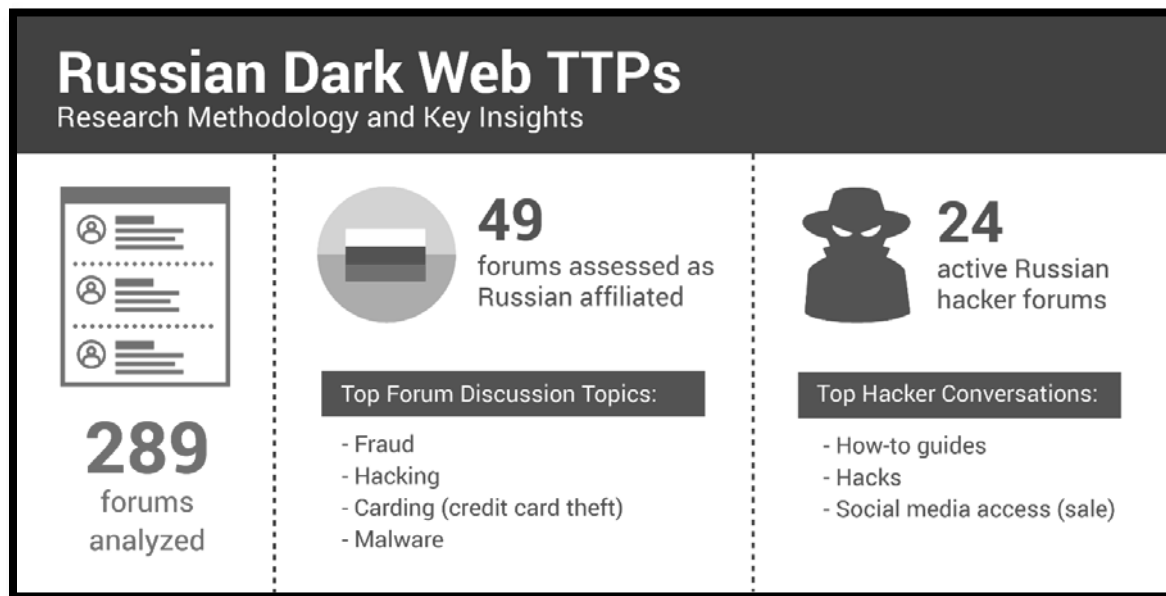


Image 2: Russian Deep and Dark Web TTPs

We conducted manual (i.e. no automated data collection) research on 73 known Russian-affiliated Deep/Dark web forums over a period of 45 days that had 67,952 posts all centered around current events and hacking, credit card and financial fraud, fraudulent documents, cyber security, software hacks, and online gaming information. These forums are where most users go to obtain “legitimate” information regarding hacking, bitcoins, and various criminal activities.

There were two known popular Russian Dark Web forums with 3809 posts during this time period. The activity contained within these forums revolved around hacking, carding, and sales of illicit goods through Dark Web online marketplaces. Russian activity on the Dark Web has been in existence for many years, and some sites have been around so long that there is a growing interest in exploring the use of the Dark Web due to the anonymity it provides for the average security-conscious individual. Among the forums, we identified three that reasonably involved state-sponsored activity within the Deep Web. These forums contained a total of 138,325 posts during the research time period; information predominantly revolved around news and current events. One forum centered specifically on current events in Ukraine, and another specifically focused on community and business events in Sevastopol ("Sevastopol.info • Главная страница," 2016.), on the Crimean Peninsula ("PrisonPlanet Forum - Index," 2016.). Illegal and criminal activity was not found on these forums.

ISIS Cyber Deep and Dark Web Trends

From a non-state actor perspective, it is important to consider how ISIS has come to use the Deep and Dark Web, as well as how they are using the Clear Web to aid in their activities within other layers of the Internet. ISIS spent several years establishing their digital footprint on all layers of the Internet. ISIS members, supporters and affiliates, media producers, Cyber Caliphate hackers and supporters, aspiring jihadists, and potential recruits all maintain a robust presence that continues to evolve and change given the many challenges their online presence faces. ISIS began creating their digital footprint in 2011, when they appeared in forums and applied online propaganda techniques learned from Al-Qaida in Iraq. By 2013 ISIS was established and growing online. The height of ISIS' online digital campaign arrived in 2014

when they had multiple websites and their social media propaganda machines were producing professional content daily.

The hacktivist group Anonymous has targeted ISIS as part of their digital counterinsurgency movement ("Anonymous Official Website," 2016.). Anonymous consists of independent coders and activists from around the world and has established the “Ghost Security Group,” a counterterrorism organization that combats extremism on the digital front lines using the internet as a weapon. According to Ghost Security Group, “Our cyber operations consist of collecting actionable threat data, advanced analytics, offensive strategies, surveillance and providing situational awareness through constant cyber terrain vigilance” ("Ghost Security Group™ – Cyber Terrain Vigilance," 2016). They established Op-ISIS and other “Op” campaigns designed to target ISIS’s digital footprint. The hacktivist movement and the use of crowdsourcing to identify ISIS websites and online entities have resulted in the quick targeting and removal of social media accounts and Clear Web activity. ISIS doggedly continues to create new sites and accounts despite the average pro-ISIS social media account and ISIS website remaining active for less than 24 hours before being shut down. ISIS Clear Web activity is notable due to all Deep and Dark Web activity consistently pointing to the Clear Web (see Appendix for definitions).

Additionally, Anonymous targeted and took down the Deep Web forum hosted at the ansar1.info URL. Our research further investigated the network, and learned that prior to the attack the server running the site was in Ukraine at Internet Protocol (IP) address 31.41.221.158. However, the website contained a link to the website administrators. The link led to a new website: alkhelafa.eu. At the time of discovery, this website was down. The new site was registered to IP 151.80.105.170, located in France (ref: Appendix for terms).

Image 3 below highlights the various networks and infrastructure connections to further discover several affiliated sites with similar names. Particularly, we found one spelled slightly differently: www.al-khelafa.eu. This website was running and contained updates from the previous day (NOV 2016). Both sites were hosted on the same IP listed above, and the server was in Roubaix, France. We next located two mail exchange servers connected to the alkhelafa.eu domain. They were being hosted on IP 82.214.72.222 in Berlin, Germany.

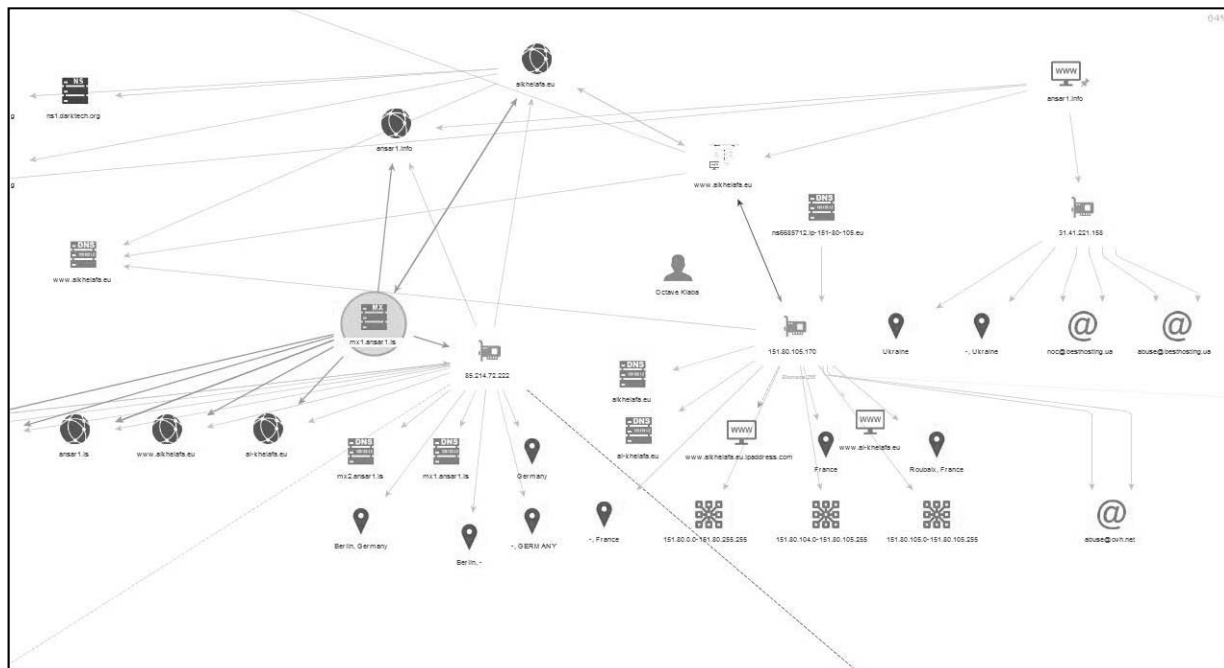


Image 3: Investigation into ansar1.info resulted into discovery of additional Deep Web Forums.

Both mail servers were also linked to the old ansar1.info domain. To clarify, the group repurposed the mail exchange servers, and simply moved the webpages to new hosted servers from Ukraine to France. The distribution of mail exchange servers and the website server indicates a distributed security methodology undertaken by the website network creators or administrators. There was no clear evidence of any direct Russian influence, but these various methods of changing – methodically – administrators, hosting services, and infrastructure

components is widely known and has been utilized extensively by affiliated Russian cyber criminals.

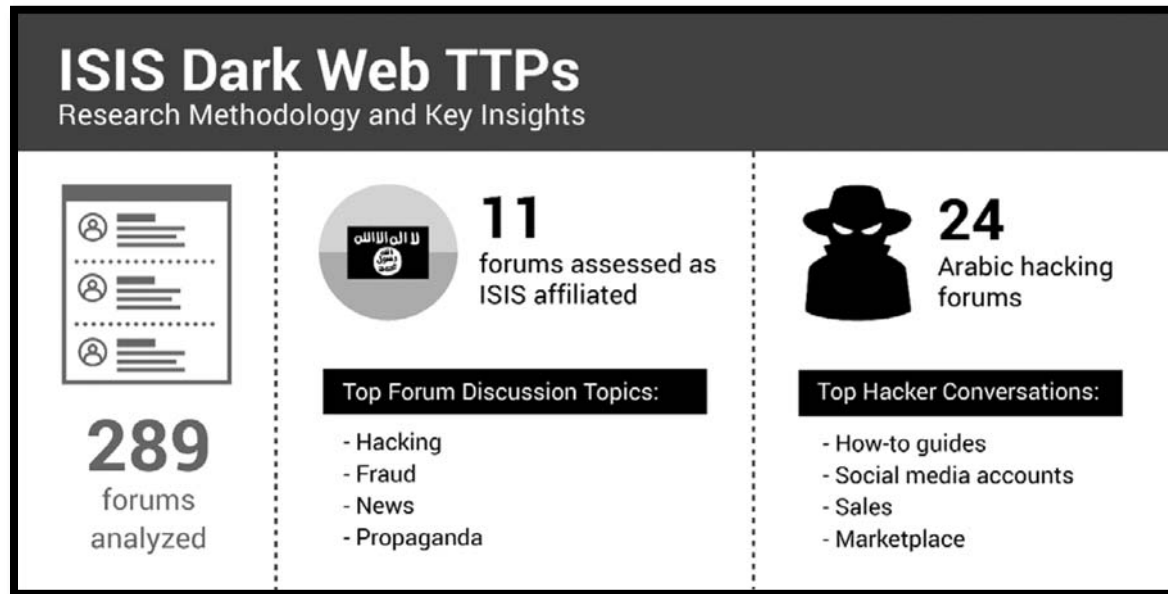


Image 4: ISIS Deep and Dark Web TTPs

During this 45 day research period, we analyzed (again, manually) 11 ISIS affiliated forums and 24 Arabic Language hacking forums. ISIS activity in the Deep Web can be summed up as forums which primarily contain many Clear Web links that lead to easily discoverable information, or extremely hard to access discussion and planning mediums (i.e. Telegram, Wickr, Dark Web user-only forums). ISIS supporters use these forums as a repository of information from vetted or known sources and posters. Analysis of ISIS's eleven active forums revealed approximately 7359 posts containing propaganda and news articles, primarily linking to the Clear Web. While there are no overt ISIS-affiliated hacking forums, activity on the Arabic language hacking forums in twelve unique Deep Web forums comprised of 17,229 posts revolving around torrents, software hacks, general hacking, malware news, and coding. There is

some Dark Web illicit activity concerning credit card fraud, and less than 1% of the information is marketplace activity and there were no dedicated Arabic Dark Web marketplaces accessed or analyzed.

Analysis of the posts on the top-tier Jihadist forums Shamikh and Manbar indicated most of their information resides on the Clear Web. All links shared on these Deep Web forms lead to external websites residing on the Clear Web in ‘digital dead-drop’ locations like JustPaste.it or Pastebin. These links are consistent with Clear Web findings, and again, they use many anonymous pasting or dumping sites to replicate and share their propaganda. It is clear ISIS actively recruits and promotes members to learn cyber skills to continue their cyber jihad, which is evident by the number of Arabic language hacking forms which primarily contain how-to publications and videos. It is also clear the call for jihadi cyber skills resulted in an increase of motivated learners in the Deep Web forums, as they understand that it is much more difficult to monitor. These forums are also a medium through which ISIS have learned and adopted known TTPs and call them their own.

ISIS activity on the Dark Web is minimal despite claims by Google that they are being pushed towards operations on this layer of the internet (Vitaris, 2016). There is an interest in moving to the Dark Web with the number of YouTube videos being published in Arabic that cover the basics on how to use Tor and how-to guides on the Dark Web. ISIS affiliates have expressed concerns with the Deep Web forms based on the amount of forbidden content, such as porn and drugs, which make the Dark Web something to be avoided or used sparingly. There are no direct links indicating ISIS is conducting illicit or criminal activities such as weapons sales on the Deep or Dark Webs.

In November 2015, ISIS established their first Dark Website entitled “Isdarat.”

Controversy surrounded this site after it was taken down by Anonymous and further exploitation was conducted on this site. Upon examination the logs associated with this Dark Website held information for DarkZhyk, a known Russian Keylogger containing a Remote Access Trojan (RAT), which points to possible Russian influence; however, the IP address associated with this website was 25.154.73.36, which belongs to the United Kingdom’s Ministry of Defense (29 / November / 2015 / *Krypt3ia*, 2015). This led to the questioning of the validity of this Dark Web activity truly being owned by ISIS (see Appendix for definitions).

An older Al-Qaida Dark Website entitled “Jihad Archives” was discovered; analysis of this site indicated it was in use from 2008 through 2012 (“Jihad Archives,” 2012). This site contains over 5000 files covering a variety of personas, information on Afghanistan, Somalia, September 11th, Arab Spring Publications, and others. The United Cyber Caliphate promoted this website on their Telegram Channel on September 6th, perhaps with the end goal of it being repurposed for ISIS media and propaganda, or perhaps seeing this as a means to have a stable presence on the Dark Web (“Pro-ISIS Cyber Kahilafah Hacking Group Previews Jihad Archives On The Darknet On Telegram | The Cyber & Jihad Lab,” 2016).

An additional site, “Muslim News,” was discovered on the Dark Web (“Muslim News,” 2016). This website contains no direct indicators linking it to be an actual ISIS website. Examination of this site reveals all links shared lead to external websites hosted on the Clear Web. These links are consistent with independent Clear Web searches. Given the simplicity of these sites, and that all links are external indicate ISIS may not yet have the capability to establish and adequately host a website on the Dark Web (08 / August / 2016 / *Krypt3ia*, 2016).

Who is the United Cyber Caliphate?

The types of activities each of these groups conduct within the Deep and Dark Webs have some similarities but vary in expertise and intent. When examining capabilities of Russian state-sponsored actors, as well as non-state sponsored actors, we find they are exceptionally capable and quite sophisticated in the cyber realm (Hellmann, 2016). The Russian capability is known to be an extension of their intelligence services and active around the world but (based on open source, it is pure speculation and conjecture, with very little solid and technically backed evidence) it is possible Russia's greatest weapon may be its hackers (Matthews, 2015). ISIS and the United Cyber Caliphate (UCC) on the other hand neither have a strong cyber capability, nor state-sponsorship backing their attempts to expand their expertise.

First appearing in 2014, The Islamic State Hacking Division (ISHD) was led by Junaid Hussain, a known British hacker who, pledging allegiance to ISIS, was killed during an airstrike in 2015. ISHD claimed responsibility for several hacks and U.S. kill-list publications (Stalinsky & Sosnow, 2015). Today they are better known as the UCC and are considered to be “the ISIS hacker wing” despite the lack of evidence indicating the UCC is a professional hacking organization (see Appendix for definitions).

After Junaid Hussain's death, by March 2016, the group appeared to be sub-divided into four divisions: Ghost Caliphate Section; Sons Caliphate Army; Cyber Caliphate Army; and, Kalachnikov E-security team (Smith, 2016). In April 2016, these four groups united under one banner and named themselves the “United Cyber Caliphate.” UCC activity consists of decentralized activity with controversy surrounding the UCC due to the lack of proof suggesting ISIS leadership established the UCC to conduct cyberattacks. As noted throughout, there is continued suspicion of Russian backing of the UCC in order to create a false flag (Gilbert, 2015).

The controversy surrounding Russian involvement and the use of the UCC as a false flag surfaced in June of 2016 when Der Spiegel, a German-based news agency, first released their story citing German Intelligence as their source. The allegation of Russia conducting False Flag operations was not surprising as Russian Intelligence Services excel at such activity ("Cyber Caliphate or Kremlin False-Flag? | iHLS Israel Homeland Security," 2016). However, this allegation is unsubstantiated from publicly available information as there are no indications—technical or otherwise—the groups are tied.

Plausible deniability, and perhaps weak or vacillating Western responses, offers Russia an opportunity to exercise methods, demonstrate capability, and incite fear. In the case of the United Cyber Caliphate, deniability allows the Russians to misdirect attention, while possibly preparing to execute their plans while the West is not paying attention and focused on the false flags.

It is also plausible Russian actors may find it useful to persuade those with actual ties to ISIS to engage in concerted attacks on Western targets. Russian intent may be to direct resources and attention away from their activities, to test Western defenses and to provide the capacity to conduct a larger scale attack or provide cover to more serious espionage attempts. The UCC lacks the sophistication Russian backing would provide should this claim be substantiated (Schindler, 2016).

In early October 2016, the United Cyber Caliphate established a page on Zeronet, which is virtually impossible to take offline at this point; however, the authenticity of this page remains undetermined due to the lack of information available. The UCC's use of this Dark Web technology is notable as it is an indicator the UCC is advancing their cyber capabilities.

Additionally, the UCC uses this specific Dark Web technology because of the difficulty associated with conducting DDoS attacks targeting ZeroNet sites (ref: Appendix for definitions).

Conclusion and Summary

Russian language Dark Web activity is more prominent than any discovered Arabic language activity. There are no discoverable Arabic language forums of any type on the Dark Web; however there are a significant number of Arabic Language Deep Web forums. ISIS, using primarily Arabic as their primary language by which to communicate, has a very limited cyber capability and limited presence on the Dark Web. The vast majority of Islamist propaganda, messaging, and recruiting along with other activity can be readily found on the Clear Web (Bean, 2015).

We can assess with confidence ISIS is attempting to grow its cyber capability to mirror that of the Russian cyber actors, specifically the trolls on the Clear Web. ISIS-affiliates are emulating this activity by establishing Facebook and Twitter entities who appear to be bots rather than real human beings, and are adjusting smoothly and with effectiveness to the various efforts to “delete or purge” these accounts by the domain providers. Most of those profiles are used to retweet messages and to exchange mini-URLs or dump site addresses. There seems to be no bilateral communication going on between the ISIS profiles and the Russian troll army. However, the use of social media to create a common theme, unite like-minded individuals, harass Western countries, and establish command and control communication centers are all activities both the Russians and ISIS participate online.

Despite differences between Russia and ISIS, there are multiple forums on the Deep Web, in nearly every language, that focus on hacking and the exchange of hacking information.

There is a strong desire of both groups to improve their hacking skills. The Russians are not as vocal online about their hacking skills as are ISIS and the United Cyber Caliphate. Instead, the Russians monitor what the rest of the world is claiming they have done by posting publicly available news media stories about their successes, while perhaps assisting or using other groups, such as ISIS, as a scapegoat to cover their tracks. ISIS-affiliated entities, on the other hand, are actively exchanging and sharing information within their hacking forums. The United Cyber Caliphate has no discoverable presence on the Deep or Dark Web; their activity has been located on the Clear Web.

It may be important to note that with the steady rise of Islamist activity around the world and related condemnation-like communications on the Internet, hackers worldwide have vowed to take on the fight against radicalism, in some cases joining forces with hacktivist groups such as Anonymous. However, there is no evidence of Russian social media activity directly targeting ISIS or evidence of Russians participating in any of these hacktivist movements. This absence of information or Russian dialogue coordinating attacks against ISIS online strains credulity to the point of impossibility. Given the known ability of Russia's formidable cyber capabilities, the lack of activity targeting ISIS or other terrorist groups that are within the Russian areas of interest such as the rise of the Chechen Islamists, specifically those who have sworn allegiance to ISIS is surprising. No communications were discovered on the Deep and Dark Web regarding this topic and nothing has surfaced on the Clear Web.

ISIS on the other hand is loud and currently unsophisticated in hacking. Nevertheless, ISIS capabilities are growing and we witnessed several threads calling for lone-wolf actors to learn hacking skills on the Deep Web; the threads provided links to Clear Web information and classes. It is evident ISIS cyber actors have mastered social media as a command and control

communicative platform and one from which to launch effective hearts and minds operations on the Clear Web. ISIS activity on the Deep Web is limited to the sharing of TTPs and dissemination of Clear Web links. They have a limited Dark Web capability that once again points immediately to the Clear Web, which indicates ISIS is attempting to move to the Dark Web, but lacks the sophistication required to maintain a presence of forum at this time.

The presence of ISIS actors on mobile applications should remain a focus as they use these channels to publish propaganda and links to websites that would otherwise immediately be taken offline, or be subjected to rapid account suspension and content deletion. ISIS' desire for a permanent digital online presence is evident in the redundancy in which they publish and push their propaganda on multiple websites and social media platforms. The multiple website approach is the only means to ensure their propaganda has a better chance of reaching the intended audience to promote their message and agenda. A large portion of ISIS data also resides on the Deep Web accessed via Telegram and WhatsApp, mobile applications (apps) which offer peer to peer encryption. Apps such as these are easier to maintain since they are not immediately subjected to cyber-attacks and Terms of Service violations.

While there is evidence ISIS cyber actors passively monitor Russian cyber actors in the Deep and Dark Web, there is no evidence of direct communication between the two entities. The desire to maintain anonymity on the Internet, protect individual identities while spreading propaganda, and conduct massive disinformation campaigns to influence global events is a common denominator between the two groups.

Indications of ISIS' passive observance of Russian Deep and Dark Web TTPs exist in loose, indirect ways. This existence was only identified by first studying both the TTPs of how Russian actors and ISIS-affiliated actors use the Deep and Dark Web independently, then

assessing the convergence of TTPs. A remaining outlier is the Cyber Caliphate. Mainstream media appears to project the message the United Cyber Caliphate is not related to ISIS, but is rather backed by either Russian Hackers or Russian State Sponsored cyber criminals as part of a global campaign. However, our research provided no evidence to support the Der Spiegel claim, or any other mainstream media claim, identifying direct ties between Russia, state-sponsored or not, and the United Cyber Caliphate. It is possible media stories supporting this theory represent a disinformation campaign in and of itself, or that certain behavior mimics attributed Russian activity.

References

- 20 | June | 2016 | intelNews | “Islamic State’s online army is a Russian front, says German intelligence” | (2016, December 8). Retrieved from <https://intelnews.org/2016/06/20/01-1921/>
- 08 | August | 2016 | Krypt3ia [Web log post]. (2016, August 8). Retrieved from <https://krypt3ia.wordpress.com/2016/08/08/>
- 29 | November | 2015 | Krypt3ia [Web log post]. (2015, November 29). Retrieved from <https://krypt3ia.wordpress.com/2015/11/29/>
- Anonymous Official Website. (n.d.). Retrieved from <http://anonofficial.com/>
- Barron, J. (1974). John Barron: Dezinformatsiya: The KGB’s Disinformation Activities. Retrieved from <http://www.heretical.com/miscella/dinform.html>
- Bean, D. (2015, August). How ISIS Made Twitter One of Its Main Recruiting Tools - And What Can Be Done About It. Retrieved from <http://ijr.com/2015/08/380544-how-isis-made-twitter-one-of-its-main-recruiting-tools-and-what-can-be-done-about-it/>
- Chen, A. (2015, June 2). The Agency - The New York Times. Retrieved from <http://www.nytimes.com/2015/06/07/magazine/the-agency.html>
- Cyber Caliphate or Kremlin False-Flag? | iHLS Israel Homeland Security. (2016, June). Retrieved from <http://i-hls.com/2016/06/cyber-caliphate-or-kremlin-false-flag/>
- Dayspring, S. M. (2015, December). Toward a theory of hybrid warfare: The Russian conduct of war during peace. Retrieved from http://calhoun.nps.edu/bitstream/handle/10945/47931/15Dec_Dayspring_Stephen.pdf?sequence=1

- Dishman, C. (2016, October 25). 6 Terrorist and Criminal Dynamics: A Look Beyond the Horizon. Retrieved from <http://cco.ndu.edu/News/Article/980805/6-terrorist-and-criminal-dynamics-a-look-beyond-the-horizon/>
- Ghost Security Group™ – Cyber Terrain Vigilance. (n.d.). Retrieved from <https://ghostsecuritygroup.com/>
- Gilbert, D. (2015, June 11). Why Kremlin-backed Russian hackers blamed Isis for cyberattack on TV5 Monde. Retrieved from <http://www.ibtimes.co.uk/why-kremlin-backed-russian-hackers-blamed-isis-cyberattack-tv5-monde-1505629>
- Hellmann, J. (2016, September 11). CIA director warns of 'sophisticated' Russian hacking capabilities | TheHill. Retrieved from <http://thehill.com/blogs/blog-briefing-room/news/295344-cia-director-russia-has-sophisticated-cyber-capabilities>
- Jihad Archives. (2012). Retrieved from agjz2ppagqsm2cg.onion/index.html
- Matthews, O. (2015, May 7). Russia's Greatest Weapon May Be Its Hackers. Retrieved from <http://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html>
- Muslim News. (2016). Retrieved from <http://ou7zytv3h2yaosqq.onion>
- Polyanskaya, A. (2003, April 30). The Virtual Eye of Big Brother. Retrieved from http://www.vestnik.com/issues/2003/0430/win/polyanskaya_krivov_lomko.htm
- Priest, D., Nakashima, E., & Hamburger, T. (2016, September 5). U.S. investigating potential covert Russian plan to disrupt November elections - The Washington Post. Retrieved from http://www.washingtonpost.com/world/national-security/intelligence-community-investigating-covert-russian-influence-operations-in-the-united-states/2016/09/04/aec27fa0-7156-11e6-8533-6b0b0ded0253_story.html

PrisonPlanet Forum - Index. (n.d.). Retrieved from <http://forum.prisonplanet.com/index.php>

Pro-ISIS Cyber Kahilafah Hacking Group Previews Jihad Archives On The Darknet On

Telegram | The Cyber & Jihad Lab. (2016, September 9). Retrieved from

<http://cjlaboratory.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/pro-isis-cyber-kahilafah-hacking-group-previews-jihad-archives-on-the-darknet-on-telegram/>

Schindler, J. R. (2016, June 18). False Flags: The Kremlin's Hidden Cyber Hand | Observer.

Retrieved from <http://observer.com/2016/06/false-flags-the-kremlins-hidden-cyber-hand/>

Sevastopol.info • Главная страница. (n.d.). Retrieved from <http://forum.sevastopol.info/>

Smith, C. (2016, April 28). ISIS: United Cyber Caliphate hackers and operations detailed in

report | BGR. Retrieved from <http://bgr.com/2016/04/28/isis-united-cyber-caliphate-hackers/>

Stalinsky, S., & Sosnow, R. (2015, August 21). Hacking In The Name Of The Islamic State

(ISIS). Retrieved from http://www.memrijttm.org/content/view_print/report/8714

Vitaris, B. (2016, January 25). Google: ISIS Should Be Pushed Back To Dark Web - Deep Dot

Web. Retrieved from <https://www.deepdotweb.com/2016/01/25/google-isis-should-be-pushed-back-to-dark-web/>

Appendix A

Definitions

APT28 (*acronym*) Advanced Persistent Threat 28. APT28 is a cyber espionage group with suspected ties to the Russian Intelligence Services. Also known as Fancy Bear, Pawn Storm, Sofacy Group, Sednit and STRONTIUM.

Carding (*term*) is a term describing fraudulent act of trafficking of credit card, bank account and other personal information online.

Clear Web (*term*) The Clear Web is the layer of the Internet which most of us are familiar with, this is publicly accessible web pages that are largely indexed on various search engines. This layer is also known as the Surface Web.

Crowdsourcing (*term*) Crowdsourcing is the act of obtaining information by enlisting the services of a number of people, paid or unpaid, typically via the Internet.

Dark Web (*term*) The Dark Web is the layer of the Internet that are intentionally and securely hidden from view. Special software and browser configurations are required to access the data.

DDoS (*acronym*) Distributed Denial of Service.

Dezinformatsiya (*Russian term*) Transliterated from Russian, it is the term used for disinformation campaigns, which is the act of intentionally providing false or misleading information that is spread in a calculating way to deceive audiences.

Distributed Denial of Service (*term*) A DDoS attack is a type of Denial of Service (DoS) attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack.

Deep Web (*term*) The Deep Web is the layer of the Internet that is hidden from the public. Authentication is required to access the data within.

False Flag (*term*) The term “False Flag” is used to describe cover operations that are designed to deceive in such a way that the operations appear as though they are being carried out by entities, groups, or nations other than those who planned and executed them.

Hacking (*term*) The act of hacking is to use a computer to gain unauthorized access to data in a system.

Hacktivism (*term*) The term hacktivism is the act of hacking or breaking into a computer system, for a politically or socially motivated purpose.

Hacktivist (*term*) A hactivist is the individual that performs the act of hacktivism.

I2P (*acronym*) The Invisible Internet Project.

Invisible Internet Project (*term*) The I2P network is an anonymous, peer-to-peer distributed communication network that allows access the Dark Web using a proxy.

IP (*acronym*) Internet Protocol Address.

Internet Protocol Address (*term*) This is a numerical label assigned to a device participating in a computer network utilizing the internet.

Keylogger (*term*) A Keylogger refers to software designed to monitor keyboard strokes.

ISHD (*acronym*) Islamic State Hacking Division.

ISIS (*acronym*) Islamic State in Iraq and Syria.

Jihad (*Arabic term*) An Arabic term for a holy way or crusade fought by Muslims to defend their spiritual beliefs.

PAI (*acronym*) Publicly Available Information.

Proxy (*term*) In computer networks, a proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers.

RAT (*acronym*) Remote Access Trojan.

Remote Access Trojan (*term*) This term refers to a malware program that includes a backdoor administrative control over the target computer.

Sofacy Group (*term*) The Sofacy Group is a cyber espionage group with suspected ties to the Russian Intelligence Services. Also known as Fancy Bear, Pawn Storm, APT28, Sednit and STRONTIUM.

The Onion Router (*term*) Also known as TOR. It is a free software and open network that helps maintain anonymity and allows access to the Dark Web's .onion websites.

TOR (*acronym*) The Onion Router.

Torrent (*term*) A torrent file is a computer file that contains metadata about files and folders that are to be distributed amongst various computers.

Troll (*term*) In Internet slang, a troll is a person who sows discord on the Internet by starting arguments or upsetting people, by posting inflammatory, extraneous or off-topic messages in an online community with the deliberate intent of provoking readers into an emotional response.

TTP (*acronym*) Tactics, Techniques and Procedures.

United Cyber Caliphate (*term*) ISIS' hacking division.

UCC (*acronym*) United Cyber Caliphate.

URL (*acronym*) Uniform Resource Locator and is a reference (an address) to a resource on the Internet.

Zeronet (*term*) Zeronet is an open, free and uncensorable network of websites using bitcoin cryptography and BitTorrent network technology.

Appendix B

Example Working Deep and Dark Web domains / onions

[DO NOT ACCESS THESE LINKS WITHOUT ADEQUATE KNOWLEDGE AND SAFETY METHODS PRIOR TO DOING SO]

Various Links:

<http://dirnxxdraygbifgc.onion/>
<http://doe6ypf2fcyznaq5.onion/>
<http://oniichanylo2tsi4.onion/>
<http://oek4nfanuw4dccid.onion/>
<http://torlinkscqquz7bi.onion/>
(8Chan) <http://oxwugzccvk3dk6tj.onion/index.html>

Search Engines:

Torch Search: <http://xmh57jrznw6insl.onion/>
Hidden Wiki: http://wikitorewogtsifs.onion/index.php/Main_Page
Hidden Wiki: http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page
Hidden Wiki: <http://hdwikicorldeisiy.onion/index>
Daniel's Site: <http://tt3j2x4k5ycaa5zt.onion/onions.php>
Undernet Directory: <http://underdj5ziov3ic7.onion/>
Not Evil: <http://hss3uro2hsxfogfq.onion/>
OnionDir: <http://auutwvpt25zfyncd.onion/>

Russian Marketplaces:

<http://russianyhluysk53.onion/>
rusilkusru6f57uw.onion
<http://rutorec6mqdinc4cz.onion/>
<http://ramp5bb7v2abm34a.onion/login.php>

Marketplaces:

<http://drugs4ynx74xribs.onion/>

Market Comparison:

<http://deepdot35wvmeyd5.onion/dark-net-market-comparison-chart/>

Hacker For Hire:

6iv5kjosuivs6fcp.onion
<http://2ogmrlfzdnwkez.onion/>

Electronics:

<http://electrotev3tgo2p.onion/>

Forums:

<http://rhe4faeuhjs4ldc5.onion/index.php>

<http://bodytomind5hq15r.onion/>
<http://rrcc5uuudhh4oz3c.onion/>
<http://svoboda2ncbezafa.onion/sign-up/>
<http://fbcy5ylyoeqzqzcr.onion/>

Fraudulent IDs and Passports:

<http://passporxakpmzurx.onion/>
<http://xfnwyig7olypdq5r.onion/>

Social Stuff:

Meetups in Germany:
<http://6v6q4eim5b2rrhd4.onion/>

Financial Services:

Wall Street:
<http://2walldbcngigzln0.onion/>

Bicoin Laundry--- in case they are dirty ya know
<http://laundrymy244rcwn.onion/>

Did you need a new paypal account? Get yours here!
<http://ccpalsto5gglun22.onion/>

Templar Knights!
<http://tknijuhhdg4476v1.onion/>

ISIS on the Dark Web:

<http://ou7zytv3h2yaosqq.onion/>

8Chan IS Catalog:
<http://oxwugzccvk3dk6tj.onion/islamicstate/catalog.html>

Jihad Archives: (up and down)
<http://agjz2pjpagqsm2cg.onion/>

Hacked by ISIS (old)
<http://i5rbhal2iegfqzni.onion/>

Russian Influence: The Rise of Putin and Implications for the Future

“The closer you are to Russia, the more you don’t
care about terrorism”

Jill Russell , Kings College Fellowship Program

Is Russia a Threat?

2

Russia uses overt and covert means of economic warfare, ranging from energy blockades and politically motivated investments to bribery and media manipulation in order to advance its interest and to challenge the transatlantic orientation of Central and Eastern Europe.

June 2009 Open Letter from European Leaders

Millions around the world increasingly see America not as a model of democracy but as relying solely on brute force, cobbling coalitions together under the slogan “you’re either with us or against us.”

V. Putin Op-Ed to American People

The West’s values and strategic interests and those of Russia are fundamentally incompatible.

Chatham House, The Russian Challenge, 2016



Europe During the Cold War

3



NATO 2004

4



NATO 2008

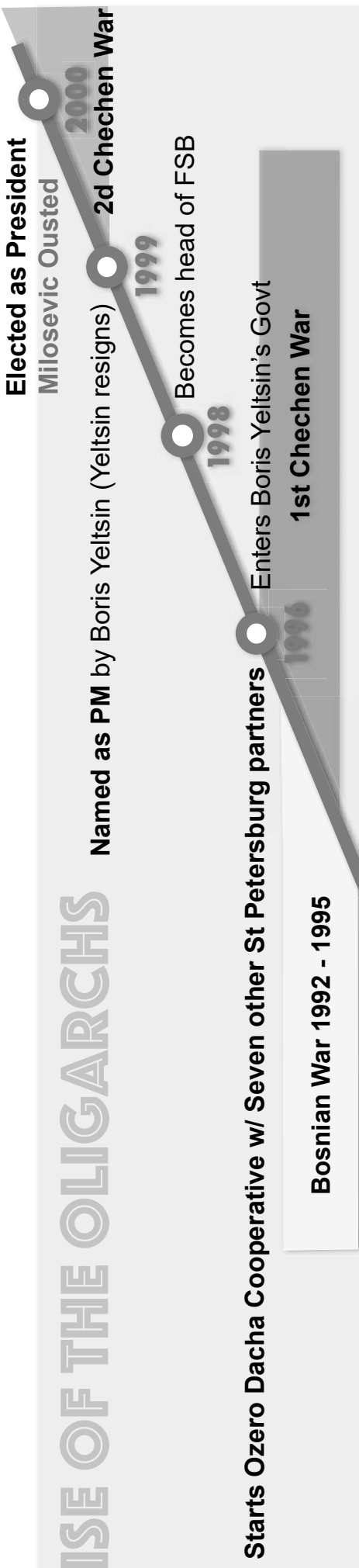
5



Putin's Timeline

6

RISE OF THE OLIGARCHS



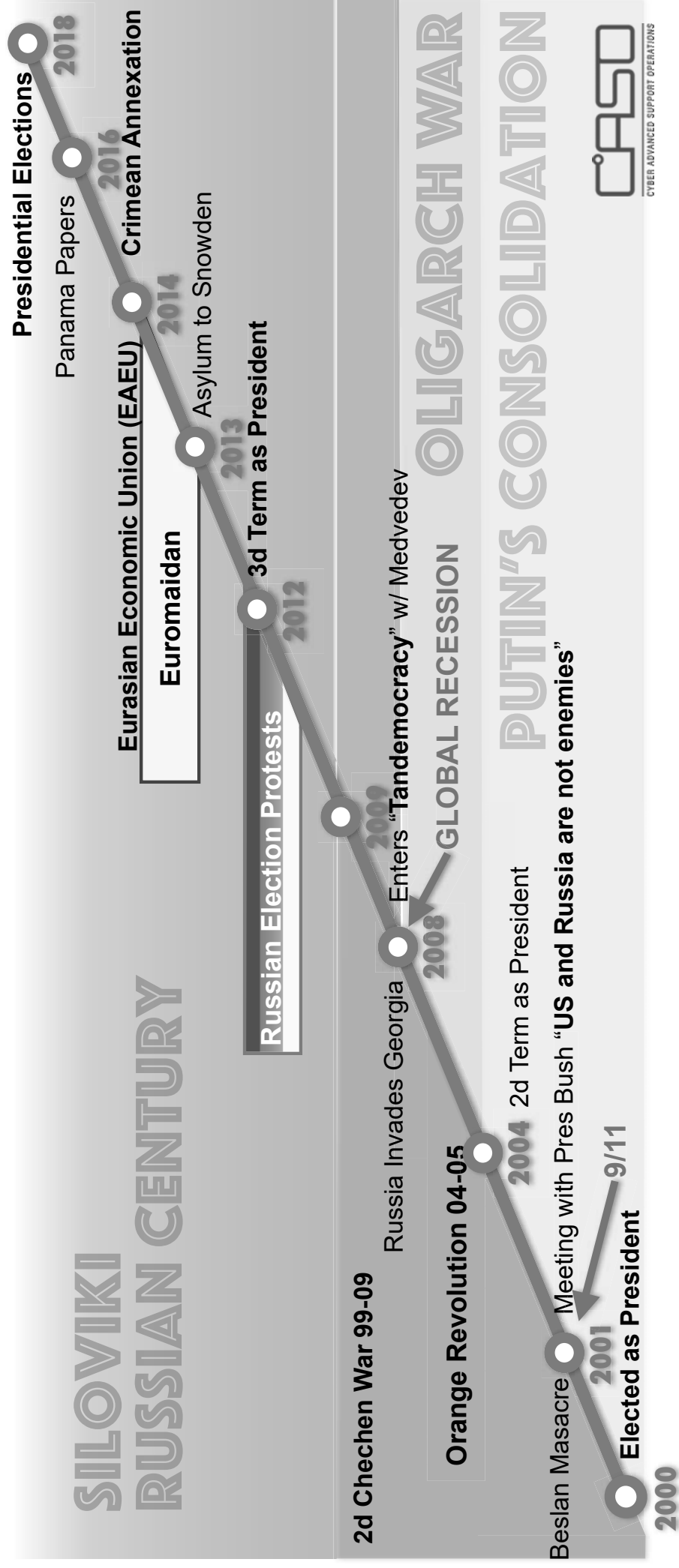
SOVIET PERIOD



CYBER ADVANCED SUPPORT OPERATIONS

Putin's Timeline

7



What Did Putin Conclude

8

- “Breakup of the Soviet Union was the greatest geopolitical catastrophe of the century.”
- Communism did not work, But neither does Liberalism
- Russia is surrounded** and must defend itself from external aggression and internal subversion.
- Trying to play by rules that were established by the West is futile
- The global security architecture (UN, NATO, etc) favors the West
- West is out to overthrow him** - likely with a “colored revolution”
- West isn't interested in considering Russia as an equal partner
- Views Security in terms of **Military, Political, Economic AND Cultural stability**

Turn From Convergence to Confrontation



Key Speeches

30 Dec 99 Millennium Speech
10 Feb 07 Munich Conf
11 Sep 13 NYT Op-ed to America
27 Oct 16 Valdai Intl address

Gene Sharp's Influence on Russian Thinking

9

"Pillars of support are institutions and sections of the society that supply the existing regime with sources of power required for maintenance and expansion of its power capacity."

Dr. Gene Sharp in *Waging Nonviolent Struggle*



Gene Sharp's Pillars of Support

Police, Military (coercive structures)
Judiciary

Bureaucracy / Specialists

Education (centers of knowledge)

Organized Religion

Media

Business (centers of economy)

CASO

CYBER ADVANCED SUPPORT OPERATIONS

Eurasianism and Novorossiya

*"The Eurasian Empire will be constructed "on the fundamental principle of the common enemy: the rejection of **Atlanticism**, strategic control of the USA, and the refusal to allow liberal values to dominate us."*

- The West (and Unipolar System) is in state of decay and world must return to Multipolar System as a **Palingenesis**
- Russia's mission is to challenge US domination of the world
- Refers frequently to Novorossiya (New Russia)
- Task [of the future] is the 'Finlandization' of all of Europe"
- One Party State necessary

Within United States:

- Fuel instability and separatism
- Destabilizing internal political processes
- Support isolationist tendencies in America

Alexandr Dugin



"Neo-Eurasian" school of political philosophy and Eurasian Mmnt

- *Foundations of Geopolitics*
- *The Fourth Political Theory*
- *Last War of the World Island*

Putin's Goals

11

DOMESTIC/COMPATRIOT

- Maintain Control of the State
- Renewed Russian Greatness
- Distinct Identity (Eurasianism)
- Ensure Internal Resiliency

INTERNATIONAL

- Alter/Reverse Euro-Atlantic Orientation
- Break US(Western) Dominance on International Order
- Restore Russian Sphere of Influence
- Erode Liberal Democratic Institutions



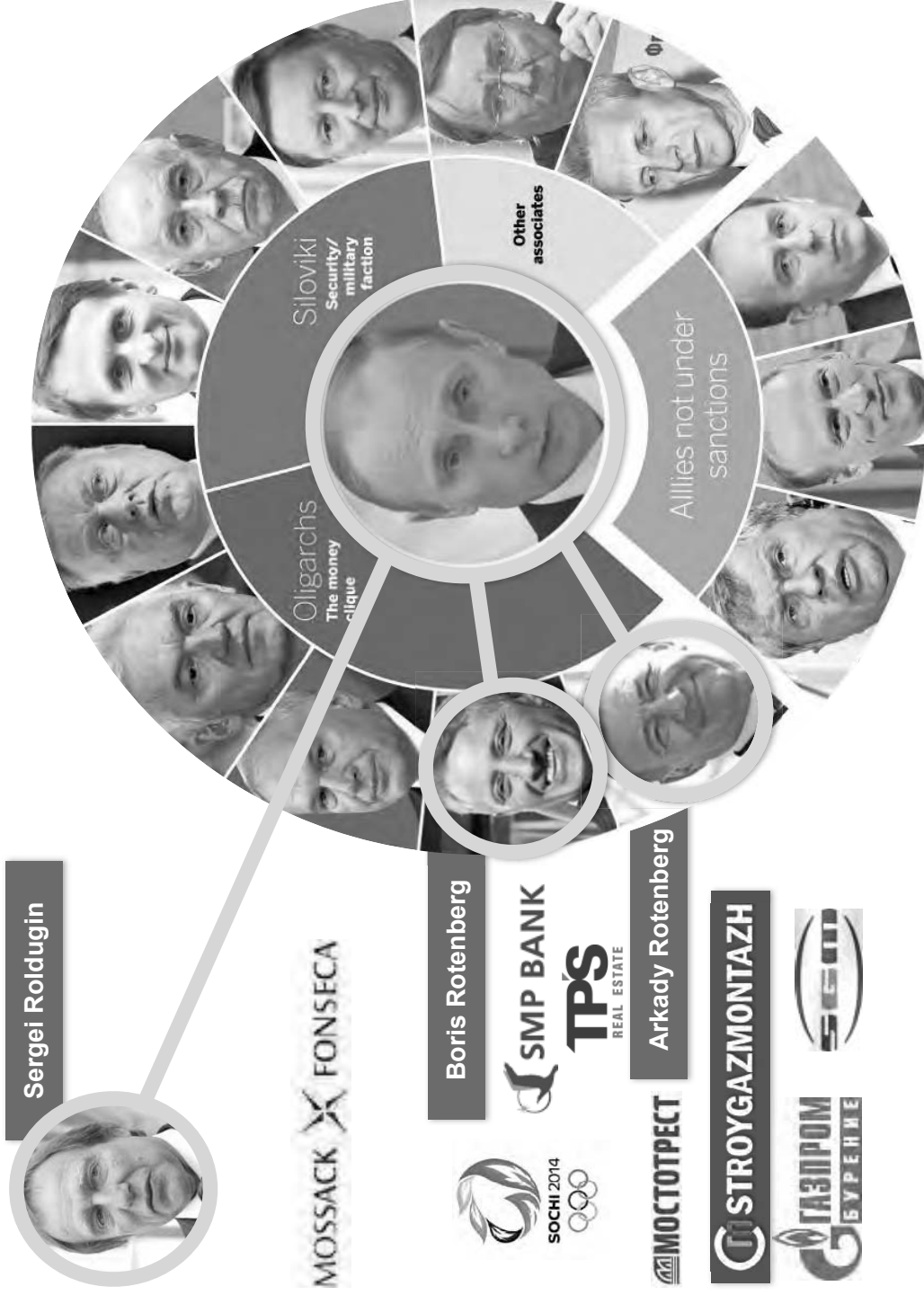
"True sovereignty... is absolutely necessary for survival'. Russia's power rests on a triad:

Renewed economic strength

The armed forces in which the administration is now investing heavily, after a long period of decline

An ideology of nationalism and patriotism, infused by history and the Orthodox Church"

V. Putin



Sergei Roldugin

The Childhood Friends

All grew up in same area of Leningrad (now St Petersburg) and remain lifelong friends.

Have significant business dealings through complex system of businesses.

Collectively hold billions in assets spanning Energy, Construction, Real Estate, Banking, Media

CASO

CYBER ADVANCED SUPPORT OPERATIONS

DOC RESEARCH
INSTITUTE

PRD Russian Railways

VEB
FOR DEVELOPMENT

Vladimir Yakunin

Viktor Myachin

COFA3
СТРАХОВАТЕЛЬСТВО

BANKROSSIYA

STRATEGIC
RESEARCH
NORTH-WEST

НАЦИОНАЛЬНАЯ
МЕДИА
ГРУППА
National Media Group

Yuri Kovalchuk

BANKROSSIYA

Vladimir Smirnov

TENEX

Nikolai Shamalov

BANKROSSIYA
Vyborg
Shipyard
GAZPROMBANK

Andrei Fursenko

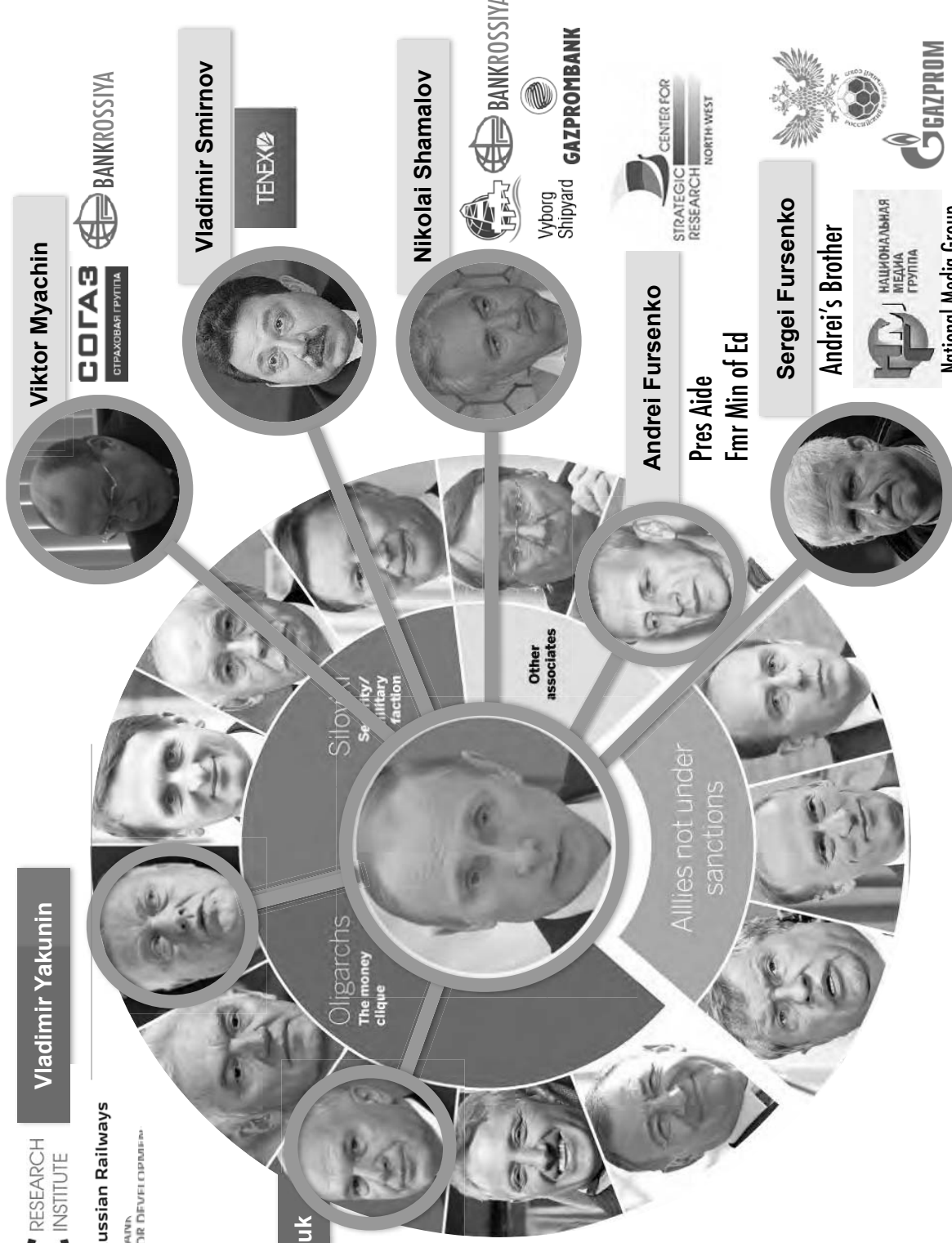
Pres Aide
Fmr Min of Ed

Sergei Fursenko

Andrei's Brother

НАЦИОНАЛЬНАЯ
МЕДИА
ГРУППА
National Media Group

GAZPROM



Ozero Dacha Collective

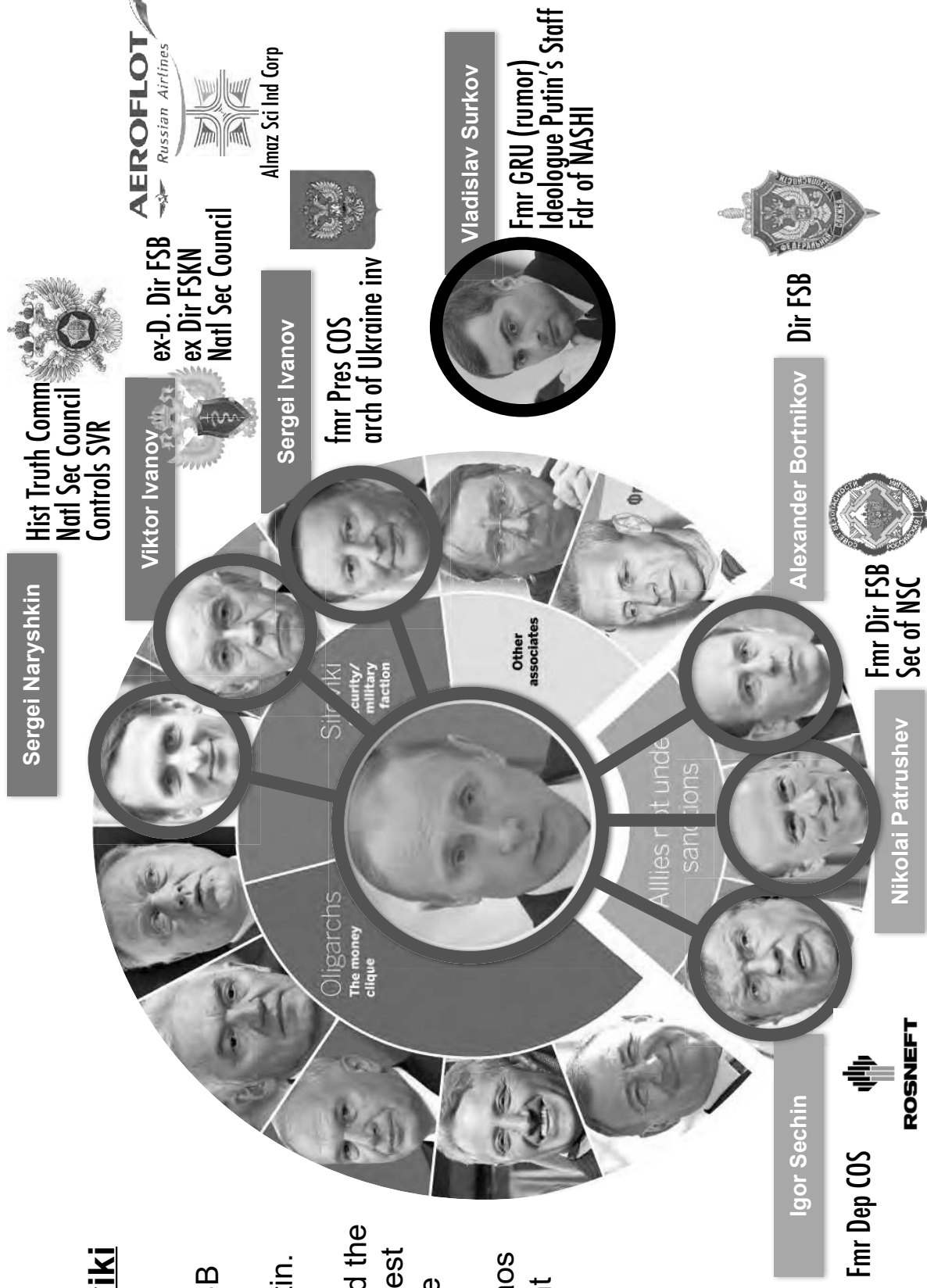
Group of Leningrad “businessmen” that developed a lake-front gated community in 1996.

The Collective holds a shared bank account which has been used as a group slush fund.

The KGB Siloviki

Group of (mostly) Leningrad KGB / FSB officers that have relationship with Putin.

Single-mindedly hold the ideology that The West caused the fall of the Soviet Union and produced all the chaos of the 2000 - present



Other Notables



Gennady Timchenko



Alexei Miller

Putin Leningrad conn
Rumored GRU conn



Yevgeny Prigozhin



Caterer
Concord Catering
Internet Research

Mikhail Lesin



Fmr Min of Press
Fmr Owner Video Int
Creator RT



Viktor Zolotov



Fed Guard Svc (FSO)
Dir Natl Guard
OMON, SOBR, Center E



Valery Gerasimov

Chief of Gen Staff
"New Generation Warfare"

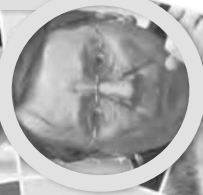


Vladimir Kolokoltsev

Min of Internal Affairs



Vladimir Kozhin



Head of Pres Property Dept



Igor Korobov

Chief GRU



Sergey Shoygu

Min Def



CYBER ADVANCED SUPPORT OPERATIONS

Kremlin Opponents Assassinated (?)

16

Yuri
Shchekochikhin



3 Jul

Anna
Politkovskaya



7 Oct

Alexander
Litvinenko



23 Nov

Natalya
Estemirova



15 Jul

Boris
Nemtsov



27 Feb

2003

2004

2006

2009

2013

2015

17 Apr



Sergei
Yushenkov

9 Jul



Paul
Klebnikov

19 Jan



Stanislav
Markelov

16 Nov



Sergei
Magnitsky

23 Mar



Boris
Berezovsky

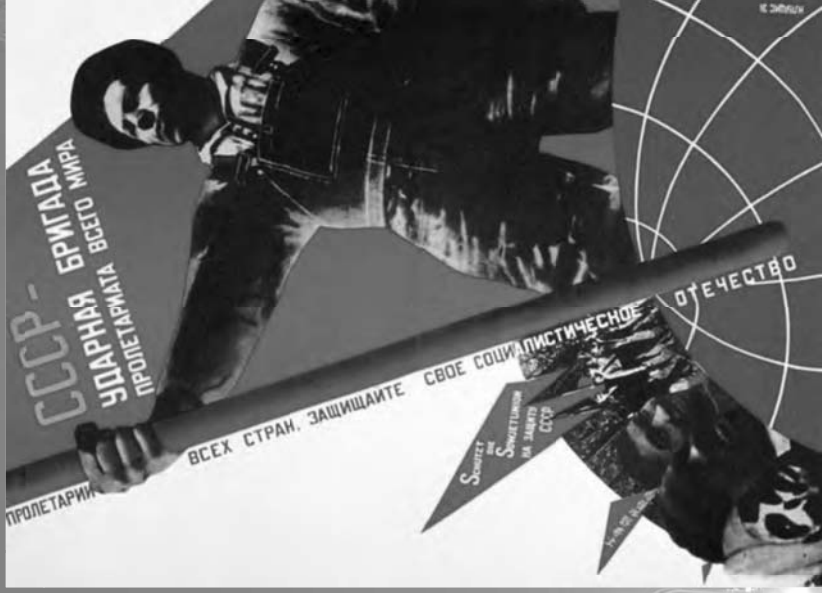
5 Nov



Mikhail
Lesin

Russian Influence & Information Struggle

17



Russian Influence Explained

18

- No real comparison in US Doctrine
- Influence is holistic and coordinated throughout
- Differences between **Political Influence** (Lavarov Foreign Ministry) and **Information Struggle** (Intelligence & Military)
- Always considers an internal and external dimension
- Presented as Strategic Defense (though offensive)
- Characterized by Strategic Patience
- Often employs win-win strategies

“The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness.”

Chief of Gen Staff Valery Gerasimov, *The Value of Science in Prediction*, Feb 2013

Active Measures in light of SM

19

ACTIVE MEASURES



Reflexive Control

Dezinformatsiya

Maskirovka

Propaganda

AGITPROP

Assassination

Political Repression

Counterfeiting

Est of Front Organizations

активные мероприятия

"the heart and soul of Soviet intelligence": "Not intelligence collection, but subversion..."
active measures to **weaken the West**, to **drive wedges in the Western community** alliances of all sorts, particularly NATO, to **sow discord** among allies, to **weaken the United States** in the eyes of the people of Europe, Asia, Africa, Latin America, and thus to **prepare ground** in case the war really occurs

KGB Maj. Gen. Oleg Kalugin

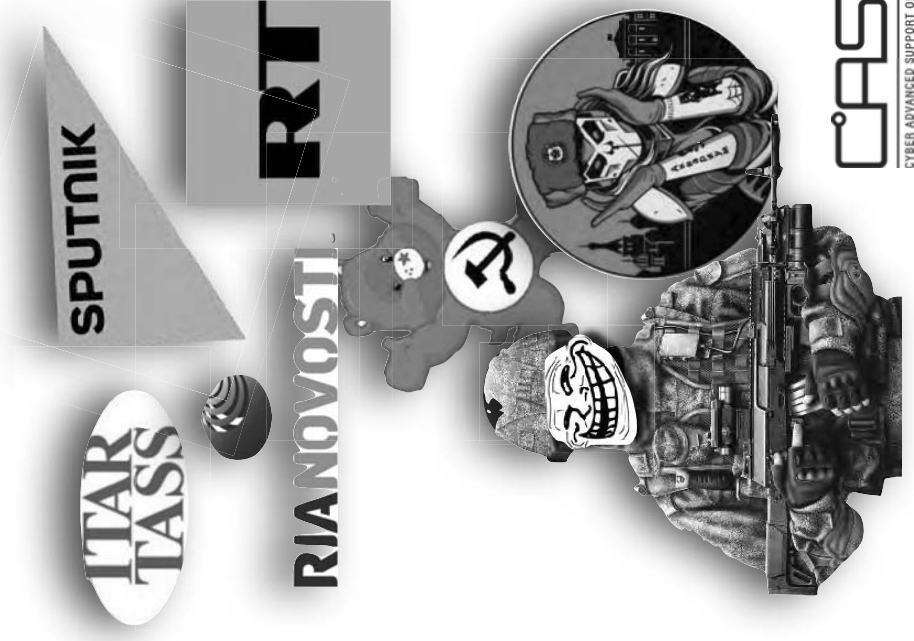
CASO

CYBER ADVANCED SUPPORT OPERATIONS

Russian investments cover:

1. **Cyber** to enable Influence
2. Internally and externally focused **media** with a substantial online presence
3. Use of plausibly deniable **social media**, discussion boards and comment pages as a force multiplier to ensure Russian narratives achieve broad reach and penetration
4. **Language skills**, in order to engage with target audiences their own language

The result is the dominant online presence now known as the **Kremlin Troll Army** and **Cyber** capabilities acting in coordination with **state-backed media**.



Influence Goals - Internal

21

GOALS

Acceptance of “Managed Democracy”
Certainty of Western hostility
Perception of Great Russia
Russian “Family Values”
Solidify Putin’s Power and Control
Resilience / Prep for war

THEMES

West is Decaying
Dysfunction of Western
“Destiny” of empire

Putin as Great Leader
Russia (and the future) is Ours
Opposing leaders are Nazis



ANNA SHUSHKOVA



GETTY IMAGES



GETTY IMAGES

Cultural and Political Resilience - Youth Programs

22



Vladislav Surkov

Fdr of NASHI



Vasily Yakemenko

Youth Organizer
Head of NASHI



Youth Democratic
Anti-Fascist
Movement
"Ours!"



Молодежное
демократическое
антифашистское
движение
«Наши»



Project Youth Network - Проект молодежная сеть

23



Artur Omarov

Head Of "Network"
Fmr NASHI



Trilateral Youth Forum



PCM

РОССИЙСКИЙ СОЮЗ
МОЛОДЕЖИ

Russian Union of Youth



BRICS

International Forum



SOURCE: PROJECT NETWORK

VICE
NEWS



Influence Goals - External

24

GOALS

Exacerbation of fractures
Reduce enthusiasm for EU/NATO
Cultivate network of Patronage
Disable Inst that combat corruption
Weaken internal Cohesion of societies
Challenge Ability of NATO/EU Response

THEMES

West is aggressor
Disfunction of West
“Destiny” of empire

Putin as Great Leader
Opposing leaders are Nazis
Russia seeks balance



Internet Research Agency - Troll Army / Trolls From Olgino

25

Agency for Internet Studies → Internet Research Agency Ltd → Internet Research

Vyacheslav Volodin

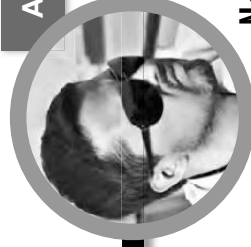
Putin Aide
Duma



Yevgeny Prigozhin



Concord Catering Company, Concord Group, Agab LLC



Alexey Soshkovets



North-Western Service Agency
Neva Entertainment

Агентство интернет-исследований



Night Wolves - Unconventional Influence

26

Alexander Zaldostanov



Path of Glory
Rally



Peace Rides



Gennady Nikulov

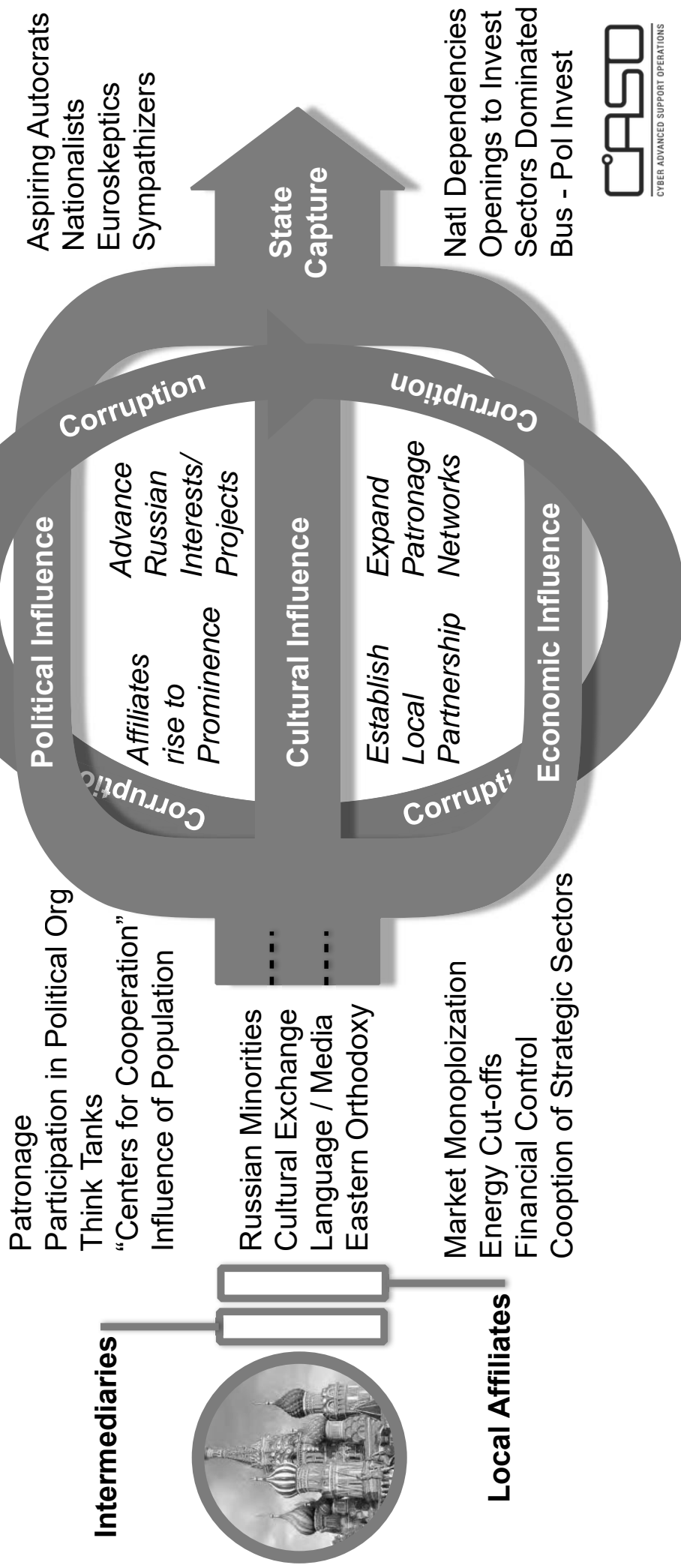


Wolf Holding
Security Structures



Channels of Russian Influence

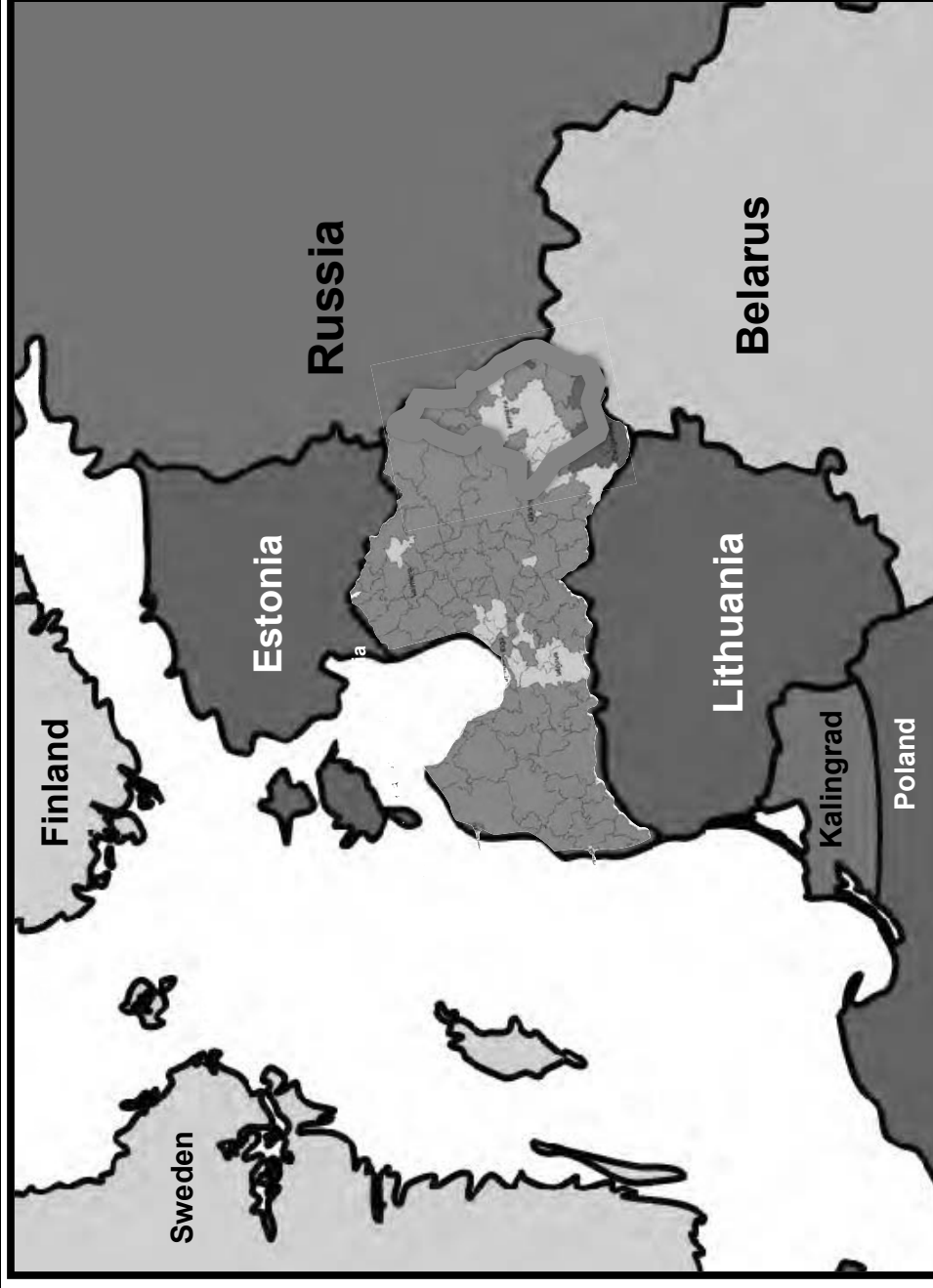
27



Case Study - Latvia

29

- **Joined NATO and EU 2004**
- **Population**
 - > 50% Russian Speakers
 - 27% Ethnic Russian
 - 10-20k Retired Russian Officers
- **50% of Bank Deposits from Russia**
- **11% of Latvian GDP from Transportation sector**
- **100% Dependent on Russian Fossil Fuel**



Insiders

Intermediaries

Local Affiliates

Case Study - Latvia

30

Sergey Lavrov



Min of For
Affairs



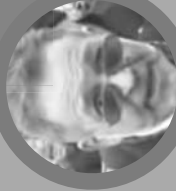
Boris Spiegel



World
Without
Nazism



Joseph Koren



Latvia
Without
Nazism



Nils Ushakovs



Harmony
Party



Aleksandr Gaponenko



NonCitizens Cong
@LVnoncitizens



VEPITSONI CONGRESS

Tatjana Ždanoka



Latvian
Russian
Union



Konstantin Malofeev



Tsargrad Group
(Media, Real estate)
St Basil Foundation



MARSHALL
capital partners



Juris Savickis

Itera Latvija
Nordeka - Trans
Fmr KGB



Vladimir Yakunin



Russian Railway



PRD
Russian Energy Logistics

RZD Logistics

Ugis Magonis



Latvian Railway



Liepaja Oil Transit
Company



Ainārs Šlesers

Fmr Min Trans



CYBER ADVANCED SUPPORT OPERATIONS

Fmr PM



Jānis Šķēle

Juta Strīke



Corruption
Prevention and
Combating Bureau



Sergei Mikhailov

Solntsevskaya
Bratva



Russian IO as IPB
Contemporary emphasis on
“informationalized warfare”
IO as both precursor and adjunct
One, two, many Crimea’s?





Russian Cyber Actors and Islamic State in Iraq and Syria

INTERACTION ON THE DEEP AND DARK WEB

Tim Newberry, CEO

tim@whitecanvasgroup.com

202-870-8216 | Fall 2016 | N0001416P3021

Research Hypothesis and Design

- Research was conducted with manual analysis and information assessment on hundreds of Deep and Dark web forums, marketplaces, and domains for a period of 45 days in October / November / December of 2016.
- Team was comprised of language, technology and operationally-focused trainers, instructors and professionals.
- Research aimed to validate open-source claims that Russia was directly related to, or by-proxy, the ISIS cyber / hacking elements known as ISHD (ISIS hacking division) or UCC (United Cyber Caliphate).

Introduction

Research results on the Deep and Dark Web conclude there are no discoverable and direct ties between Russian Cyber Actors and ISIS.

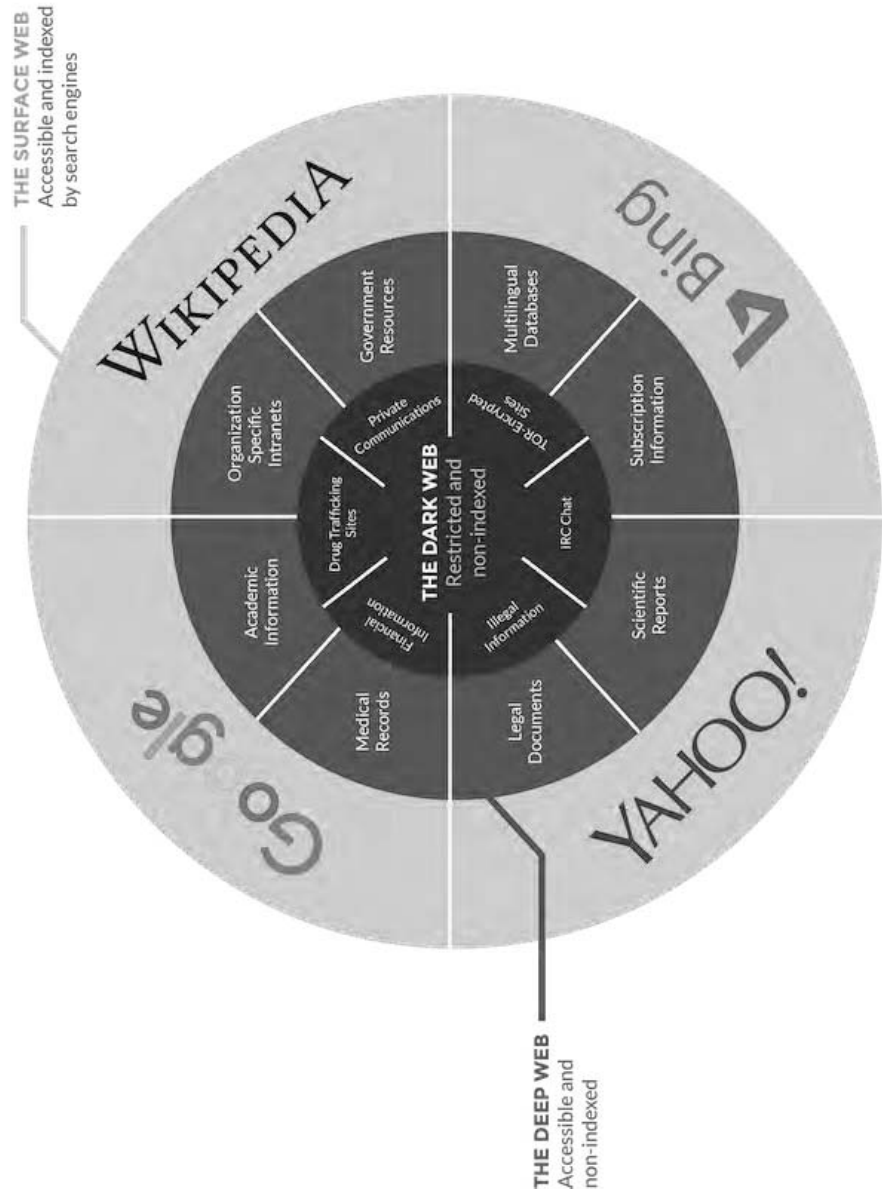
- However, there are indications that ISIS is passively monitoring Russian activity to possibly emulate Russian activity, enhance cyber skills, and establish a true United Cyber Caliphate with advanced capabilities.
- Research on this topic remains limited due to the complexity and difficulty of conducting research in the unindexed hidden layers of the Internet.

Research Methodology

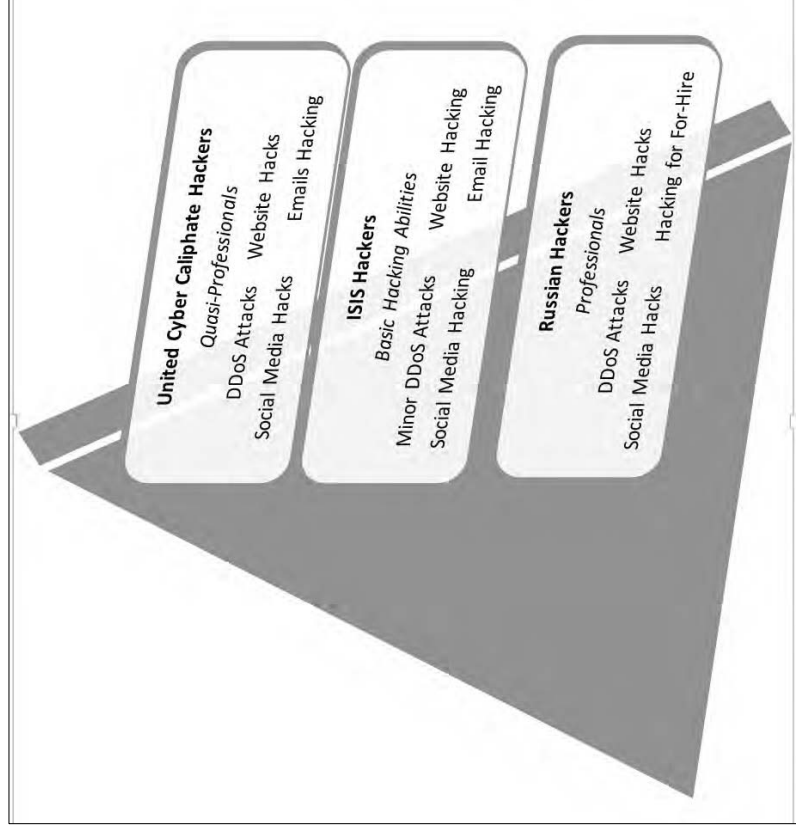
To understand if and how ISIS passively monitors Russian cyber actors in the Deep and Dark Web we must:

- Study the Deep and Dark Web TTPs of both Russian actors and ISIS-affiliated actors independently
- Assess the convergence of TTPs and how they result in an evolution of capabilities

The Layers of the Internet



Assessing the Ties Between Russia and ISIS



Similarities in activities:

- Each group has a vested interest in hacking
 - Distributed Denial of Service (DDoS)
 - Hacking email or social media accounts
 - Hacking Websites
- All three groups continue to disrupt every day activity and illegally obtain data to support their specific agendas

Russian Trolls

Home

Moments

Notifications


Messages

Search Twitter

Q

🔍

📷





TWEETS
194K

FOLLOWING
1,458

FOLLOWERS
746

LIKES
9

⚙️

👤 Follow

Alexandr Karaul'nyh
@AlexArtAndros

#Develop #IT #Web #Design #WebSite
#Builder #3D #Designer #AutoCAD
#3DMax #4D #Cinema #CryEngine
#Lumberyard #3DUnity

🌐 facebook.com/AlexArtAndros
📅 Joined October 2011



Alexandr Karaul'nyh
@AlexArtAndros · 21m

#Сводка #ЛНР #Марочко #Донбасс
#Новороссия #5октябрь2016
#Summary #LPR #Marochko #Donbass
#Novorossia #5october2016

Russian Cyber Deep and Dark Web Trends

Russian Dark Web TTPs

Research Methodology and Key Insights



289
forums
analyzed



49
forums assessed as
Russian affiliated

Top Forum Discussion Topics:

- Fraud
- Hacking
- Carding (credit card theft)
- Malware

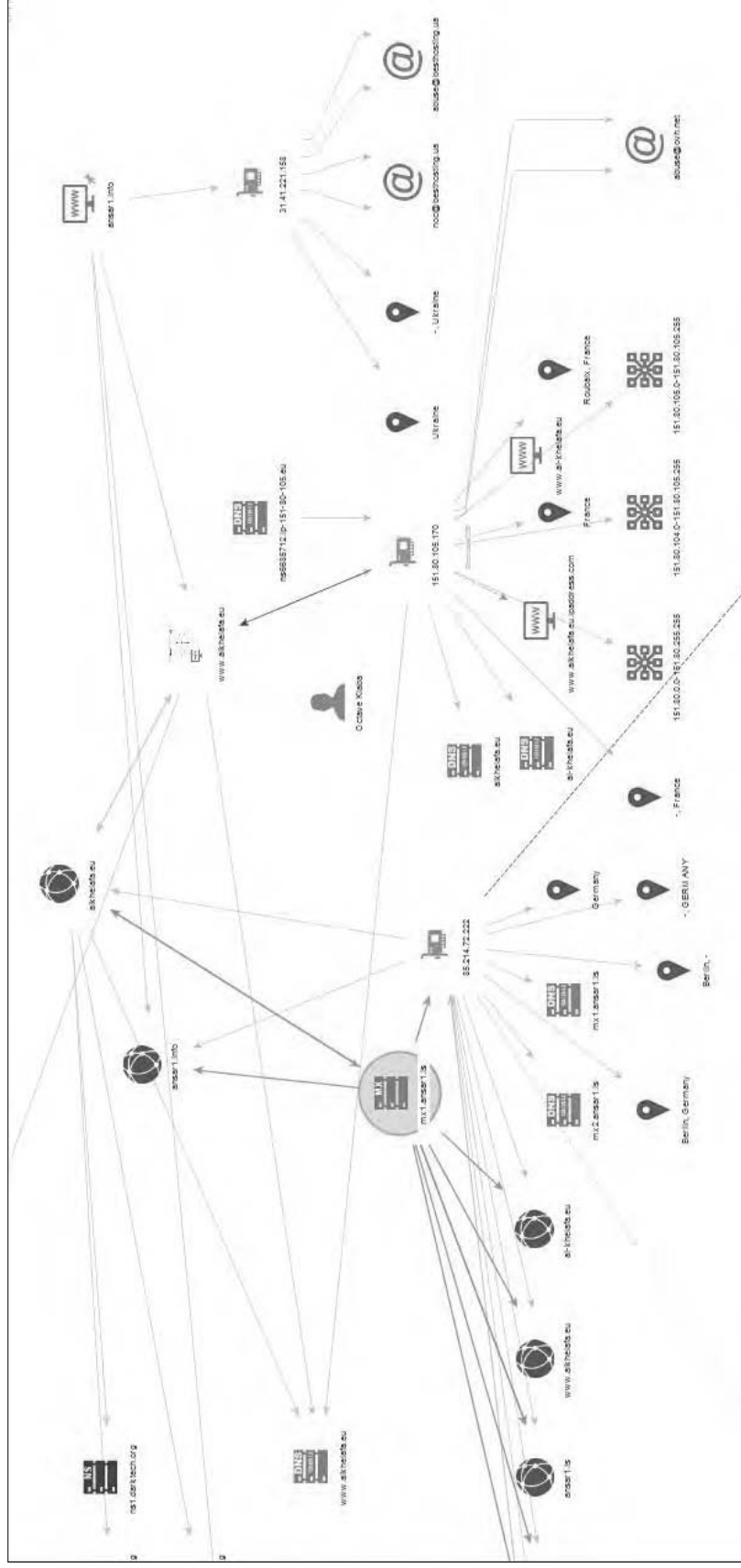


24
active Russian
hacker forums

Top Hacker Conversations:

- How-to guides
- Hacks
- Social media access (sale)

Discovering ISIS Deep Web Forums



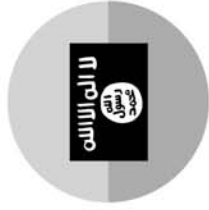
ISIS Cyber Deep and Dark Web Trends

ISIS Dark Web TTPs

Research Methodology and Key Insights



289
forums
analyzed



11
forums assessed as
ISIS affiliated



24
Arabic hacking
forums

Top Forum Discussion Topics:

- Hacking
- Fraud
- News
- Propaganda

Top Hacker Conversations:

- How-to guides
- Social media accounts
- Sales
- Marketplace

[illegible]

Assessment

ISIS is attempting to grow its cyber capability to mirror that of the Russian cyber actors, specifically the trolls on the Clear Web:

- Threads calling for lone-wolf actors to learn hacking skills on the Deep Web
- ISIS activity on the Deep Web is limited to the sharing of TTPs and dissemination of Clear Web links
- Limited Dark Web capability, that points immediately to the Clear Web; indicates a lack of sophistication required to maintain a presence of forum at this time
- Desire for a permanent digital online presence is evident based on redundancy in which they publish propaganda on multiple websites and social media platforms and use mobile applications

Information Gaps

No evidence of direct communication on the Deep and Dark Web between Russians and ISIS discovered during research

- It is possible they are communicating using different means including secret encrypted channels
- This information, if combined with other sources may provide additional links between the two groups and illuminate information regarding the United Cyber Caliphate

Conclusion

While there is no evidence of direct communication between Russia and ISIS, indications of ISIS' passive observance of Russian Deep and Dark Web TTPs exist in loose, indirect ways.

- One remaining outlier is the Cyber Caliphate. The media appears to project the message that the United Cyber Caliphate is backed by either Russian Hackers or state sponsored cyber criminals as part of a global campaign. However, our research provided not evidence to support these claims.



Tim Newberry, CEO
tim@whitecanvasgroup.com
202-870-8216